Written by: Aurel Sorin Spornic
Quang-Huy Nguyen

Odysseus
SSCD
Security Target

PUBLIC VERSION

Copyright Axalto SA – 2008.

CONTENT

Copyright Axalto SA – 2008.

Copyright Axalto SA – 2008.

Figures

Copyright Axalto SA – 2008.

1 ST Introduction

1.1 ST Identification

Title:	ODYSSEUS SSCD Security Target (Public version)
Version:	1.6 issued January 24th, 2008
Registration:	Ref. D1049311
Origin:	GEMALTO
Commercial name:	MultiApp ID SSCD
Product ref.	T1002711

The TOE is composed with:

Component	Version number	Supplier
Hardmask in ROM	1.0	Gemalto
Corrective softmask #1 in EEPROM, PDM ref. S10325940[1]	3.1	Gemalto
Micro-controller SLE66CX680PE	A13	Infineon
RMS library	2.5	Infineon
RSA2048 library	1.4	Infineon

This evaluation is done under the French scheme for Common Criteria. The certification body is the 'Direction Centrale de la Sécurité des Systèmes d'Information' (DCSSI).

1.2 ST overview

This product needs to be compliant with European electronic signature directive translated into the claimed PP [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].
So this ST focuses on the Secure Signature Creation Device, embedded in a Smart card integrated circuit.

The TOE will be designed and produced in a secure environment and used by each citizen in a hostile environment.
The product is compliant:
with Java Card 2.2.1, excepting the following restrictions:

- Logical channels are not supported
- RMI is not supported

with Global Platform 2.1.1,

[1] The softmask is a PDM item attached to the technical product T1002711.

Copyright Axalto SA – 2008.

and with IAS applet 1.01 with erratum except the following:

- the Diffie Helmann secure messaging session openning is supported in 1024 bit-long key only,
- the SHA-256 is not supported.

The SSCD security functions take advantage on the platform security functions:

- Hardware Tamper Resistance:
  - This is the chip security layer that meets PP SSVG [PP/BSI-0002].
- Secure operation of the Java Card Virtual Machine (meet PP JCS):
  - This is the Java Card Virtual Machine and Operating System that meets [PP/JCS-211], as described by [ST_ODYSSEUS-PLTF]. This sub-system insures Javacard package secure loading or deletion as well as Javacard application secure execution.

1.3 CC conformance

The compliance is assumed with CC version V2.3 (ISO 15408) ([CC-1], [CC-2], [CC-3]).
This product is a Secure signature creation device compliant to the Protection Profile CEN SSCD [PP/SSCD-TYPE2]/[PP/SSCD-TYPE2] based on a certified platform conformant to [PP/JCS-211]. This platform uses a certified chip conformant to the Protection Profile SSVG (also known as PP/BSI-0002) from Eurosmart, providing the necessary security so that value added applications can be safely loaded and executed on card without harming the electronic signature application. Therefore this ST is conformant to [PP/SSCD] Protection Profile, the platform is conformant to [PP/JCS-211] Protection Profile and the IC is conformant to [PP/BSI-0002] Protection Profile.

This ST extends CC V2.3 Part 2.
This ST is CC V2.3 conformant with Part 3 conformant and EAL4 augmented as stated in [PP/SSCD-TYPE2]/[PP/SSCD-TYPE2], [PP/JCS-211], [PP/BSI-0002].

The assurance level for this product is EAL4 augmented by:

- ADV_IMP.2 (Development – Implementation of the TSF)
- ALC_DVS.2 (Sufficiency of security measures)
- AVA_VLA.4 (Vulnerability Assessment – Analyse, Highly resistant)
- AVA_MSU.3 (Vulnerability Assessment – Analysis and testing for insecure states).

The augmentations may also be found in section §5.2.

The strength level for the TOE security functional requirements is "SOF high" (Strength Of Functions high).

Copyright Axalto SA – 2008.

1.4 References

1.4.1 External References [ER]

Reference	Title
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB-2005-08-001, version 2.3, August 2005 (conform to ISO 15408).
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2005-08-002, version 2.3, August 2005 (conform to ISO 15408).
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-2005-08-003, version 2.3, August 2005 (conform to ISO 5408).
[CEM]	Common Methodology for Information Technology Security Evaluation CCIMB-2005-08-004, version 2.3, August 2005.
[PP/SSCD-TYPE2]	Secure Signature-Creation device Protection Profile Type 2 v1.05, EAL4+
[PP/SSCD-TYPE3]	Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+
[PP/JCS-211]	Java Card System Protection Profile Version 1.0b issued August 2003, standard 2.1.1 configuration, SUN document, registered by DCSSI under PP/0304.
[PP/JCS-22]	Java Card System Protection Profile Version 1.0b issued August 2003, standard 2.2 configuration, SUN document, registered by DCSSI under PP/0305.
[PP/BSI-0002]	Smart Card IC Platform Protection Profile, version 1.0, registered by BSI in 2001 under PP-BSI-0002, Eurosmart document (SSVG Protection Profile).
[ST/INFINEON]	Security Target of SLE66CX680PE Integrated Circuit.
[FIPS 46-3]	FIPS 46-3: DES Data Encryption Standard (DES and TDES). National Institute of Standards and Technology
[SP 800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation
[FIPS 197]	FIPS 197: AES Advanced Encryption Standard. National Institute of Standards and Technology.
[RSA PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard
[FIPS 180-2]	FIPS-46-3: Secure Hash Standard (SHA). National Institute of Standards and Technology.
[CWA-ALGO]	ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures V1.1.1 (2003-03).
[ISO 7816-4]	Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange
[ISO 7816-6]	Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements
[ISO 7816-9]	Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Inter industry commands and security attributes.
[ISO 9796-2]	ISO/IEC 9796-2

Copyright Axalto SA – 2008.

Reference	Title
[JCAPI211]	Java Card™ APIs specification version 2.1.1, Sun Microsystems, Inc.
[JCRE211]	Java Card™ 2.2 Runtime Environment Specification version 2.1.1, Sun Microsystems, Inc
[JCVM211]	Java Card™ Virtual Machine Specification version 2.1.1, Sun Microsystems, Inc
[JCAPI221]	Java Card™ APIs specification version 2.2.1, Sun Microsystems, Inc, June 23, 2003.
[JCAPN221]	Application Programming Notes for the Java Card™ Platform, Sun Microsystems, Inc, version 2.2.1, October 2003.
[JCRE221]	Java Card™ Runtime Environment Specification version 2.2.1, Sun Microsystems, Inc, 2003.
[JCVM221]	Java Card™ Virtual Machine Specification version 2.2.1, Sun Microsystems, Inc, 2003.
[JVM]	The Java Virtual Machine Specification. Lindholm, Yellin. ISBN 0-201-43294-3.
[GP]	Global Platform. Card Specification – v2.1.1, March 2003.
[VOP]	Visa Open Platform Card Implementation Requirements Configuration 3 – v2.0
[IAS1]	Plateforme commune pour l' eADMINISTRATION – Spécification technique – Révision 1.01 (French document)
[IAS2]	Plateforme commune pour l' eADMINISTRATION – Spécification technique – Erratum à la version 1.01 (French document)

1.4.2 Internal References [IR]

Reference	Title
[ST_ODYSSEUS-PLTF]	**ODYSSEUS Security Target – Platform** D1049224 (ST_D1049224)
[FSP_ODYSSEUS]	**ODYSSEUS Functional Specification** D1050016 (FSP_D1050016)
[HLD_ODYSSEUS]	**ODYSSEUS High-level Design (overview document)** D1049625 (HLD_D1049625)
[LLD_ODYSSEUS]	**ODYSSEUS Low-level Design (overview document)** D1050412 (LLD_D1050412)
[IMP_ODYSSEUS]	**ODYSSEUS Implementation representation** D1050415 (IMP_D1050415)
[SPM_ODYSSEUS]	**ODYSSEUS Security Policy Model** D1050410 (SPM_D1050410)
[AUT_ODYSSEUS] [CAP_ODYSSEUS] [SCP_ODYSSEUS]	**ODYSSEUS Partial CM automation** **ODYSSEUS Generation, support and acceptance procedure** **ODYSSEUS Problem tracking CM coverage** D1049554 (ACM_D1049554)
[DEL_ODYSSEUS]	**ODYSSEUS Detection of modification** D1051233 (DEL_D1051233)
[IGS_ODYSSEUS]	**ODYSSEUS Installation, Generation and Start Up Procedures** D1050210 (IGS_D1050210)

Copyright Axalto SA – 2008.

Reference	Title
[ADM_ODYSSEUS]	**ODYSSEUS Administrator Guidance** D1050012 (ADM_D1050012)
[USR_ODYSSEUS]	**ODYSSEUS User Guidance** D1050014 (USR_D1050014)
[DVS_ODYSSEUS]	**ODYSSEUS Development Security Documentation** D1049550 (DVS_D1049550)
[LCD_ODYSSEUS]	**ODYSSEUS Life-cycle definition documentation** D1051235 (LCD_D1051235)
[TAT_ODYSSEUS]	**ODYSSEUS Documentation of development tools** D1050010 (TAT_D1050010)
[COV_ODYSSEUS]	**ODYSSEUS Analysis of test coverage** D1050664 (COV_D1050664)
[DPT_ODYSSEUS]	**ODYSSEUS Analysis of the depth of testing** D1050662 (DPT_D1050662)
[FUN_ODYSSEUS]	**ODYSSEUS Test Documentation** D1050661 (FUN_D1050661)
[MSU_ODYSSEUS]	**Odysseus Analysis and testing for insecure states** D1051227 (MSU_D1051227)
[SOF_ODYSSEUS]	**ODYSSEUS Strength of TOE security functions analysis** D1051229 (SOF_D1051229)
[VLA_ODYSSEUS]	**ODYSSEUS Vulnerability Analysis** D1051231 (VLA_D1051231)
[PERS_ODYSSEUS]	**ODYSSEUS SSCD Basic personalisation** D1051441

1.4.3 Reference of Associated Distribution Sheet

[DS_ODYSSEUS]	**ODYSSEUS SSCD Security Target Distribution sheet** D1049711

Copyright Axalto SA – 2008.

2 TOE Description

This part of the ST describes the TOE as an aid to the understanding of its security requirements.
It addresses the product type, the smart card product life cycle, the TOE environment along the smart card life cycle and the general features of the TOE.

2.1 Product type

The product is a smartcard including a plastic card and a module performing the interface between reader and the embedded chip. Other smart card product elements (such as holograms, security printing…) are outside the scope of this Security Target.
The Target of Evaluation (TOE) is the Smart Card Integrated Circuit with Embedded Software in operation and in accordance to its functional specifications.

The TOE is composed of a hardware and software platform and a signature application:

- Integrated Circuit including crypto libraries, which is certified separately according to [ST/INFINEON] claiming [PP/BSI-0002],
- GEOS Operating System,
- Card Manager & Open Platform functionalities [GP], including OP/GP API.
- Java Card Virtual Machine 2.1.1 [JCVM211], Java Card Runtime Environment 2.1.1 [JCRE211] and Java Card API 2.1.1 [JCAPI211] extended with application and object deletion functionalities from Java Card 2.2.1. The TOE follows therefore only the Java Card 2.1.1 Standard configuration according to [PP/JCS-211], as Logical channels and RMI are missing to achieve Java Card 2.2 Standard configuration as of [PP/JCS-22]. This open platform provides a firewall in order to insure application separation.
- Proprietary APIs: ISO utils, ISO Secure Messaging, File System, JavaCard extentions.
- Applications: IAS for electronic signature [IAS1], [IAS2] and possibly other Java Card applications.

The platform is based on Centaur certified platform[2] and is described by [ST_ODYSSEUS-PLTF].
The certified platform Centaur contains:

- Software modules as Card Manager, Javacard API (JCAPI), Javacard VM (JCVM), Javacard Runtime Environment (JCRE), a Generic Operating System (GEOS),
- An Integrated Circuit (IC) and its dedicated software including a crypto library.

The TSFs are composed of:

- The chip and its crypto library,
- The GEOS operating system,
- The Card Manager loader (applets and packages loading),
- The Java Card System,
- The SSCD application (as a Java Card application).

As this ST is a composition, each chapter indicates the items covered by the platform ST and furthermore by the IC security target.

Next picture represents the TOE and the TSF. The TOE does not include the applets that may be loaded post-issuance and some of the functionalities of the IAS applet. The TOE is bordered with blue continuous line.

[2] DCSSI issued certificate no 2006/08.

Copyright Axalto SA – 2008.

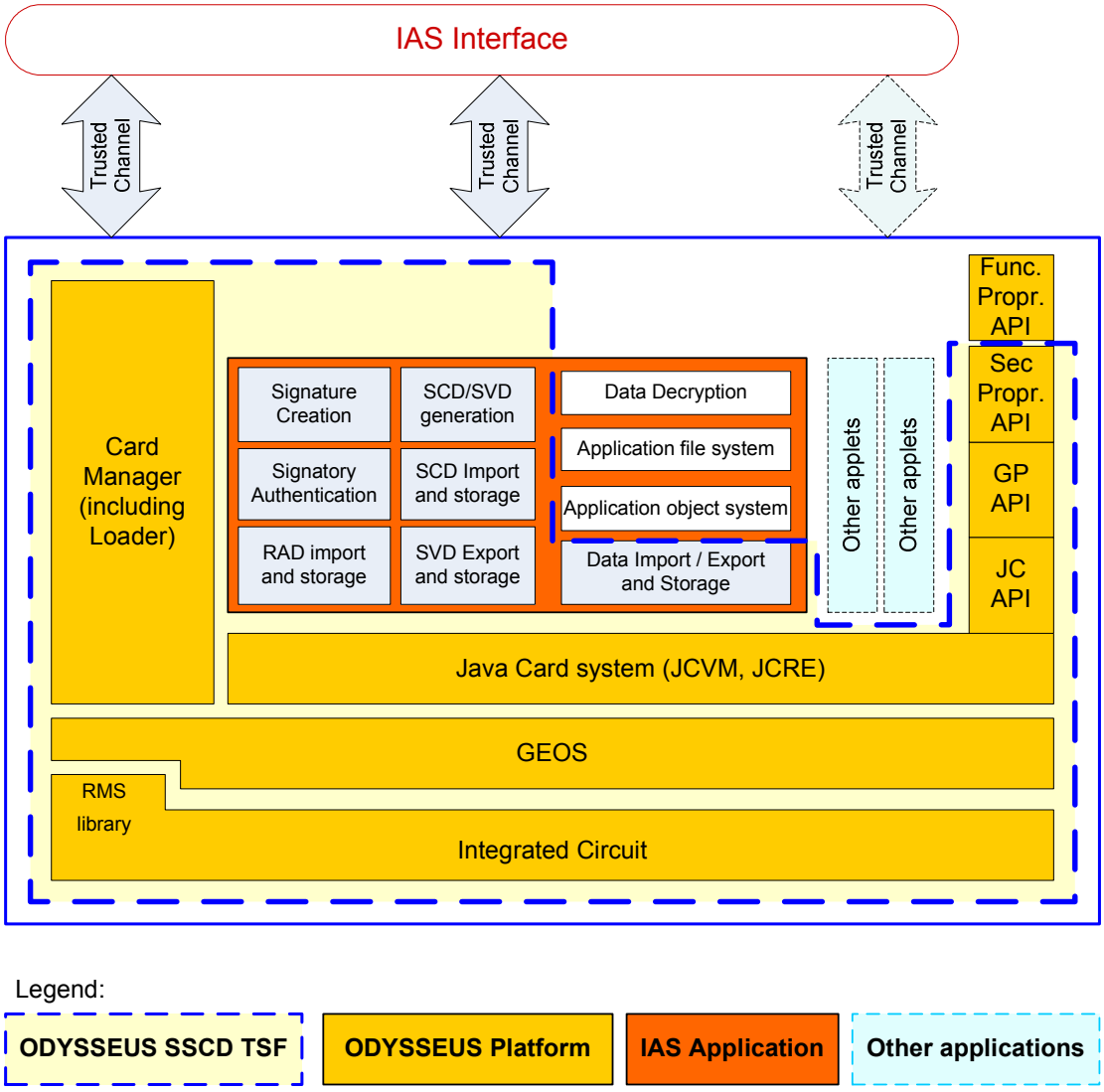

Figure 2.1 – The TOE

2.2 Product description

2.2.1 Terminology

In this document the terminology of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] is used.
The IAS application uses public key encryption. The Signature Creation Data (SCD) is the private key and the Signature Verification Data (SVD) is the public key.
The Signatory's Reference Authentication Data (RAD) is the PIN stored in the card and the Signatory's Verification Authentication Data (VAD) is the PIN provided by the user.

2.2.2 Functionalities

The IAS application provides functions necessary for devices involved in secure electronic signatures, that are included in the scope of the evaluation (part of the TSF) and some others functionalities that are not evaluated.

Copyright Axalto SA – 2008.

2.2.2.1 Evaluated services

The evaluated services or functionalities are represented in the next figure that shows Type 2 and Type 3 TOE operations as defined in [PP/SSCD-TYPE2]:

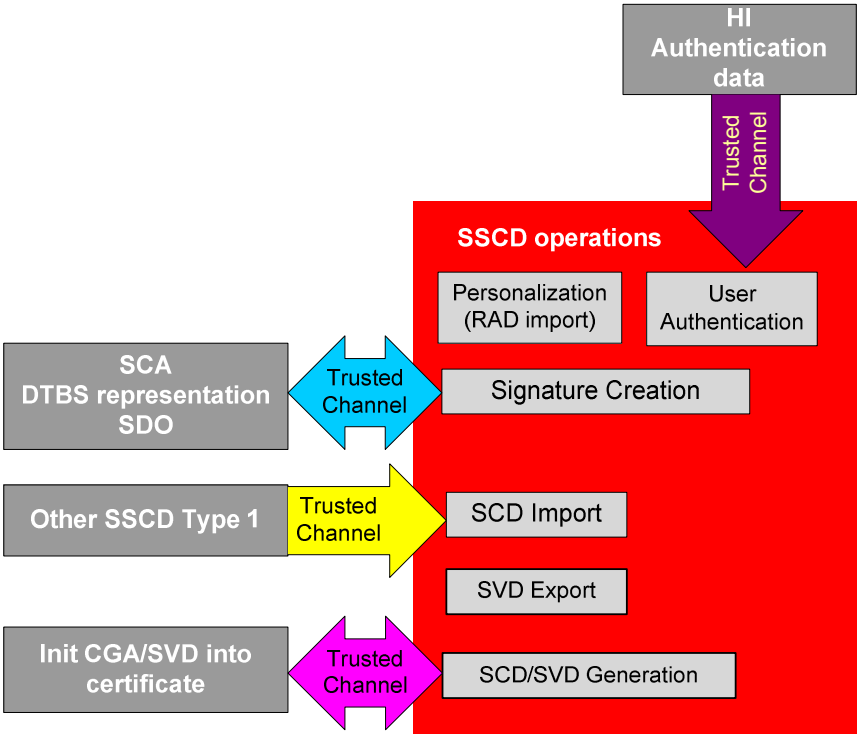

Figure 2.2 – Type 2 and Type 3 SSCD operations

1. Generate the SCD and the correspondent SVD, or Load the SCD,
2. Create qualified electronic signatures:
   (a) after allowing for the Data To Be Signed (DTBS) to be displayed correctly by an appropriate environment,
   (b) using appropriate hash functions agreed according to [CWA-ALGO] suitable for qualified electronic signatures,
   (c) after appropriate authentication of the signatory by the TOE itself,
   (d) using appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed according to [CWA-ALGO].

The TOE implements all IT security functionalities, which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SSCD the TOE provides user authentication and access control. The TOE implements IT measures to support a trusted path to a trusted human interface device. Therefore, the TOE holds Signatory's Reference Authentication Data (RAD) that is used to verify the verification data provided by the user as Signatory's Verification Authentication Data (VAD).

The TOE is initialised by importing an SCD or by generating a pair of SCD and SVD. The SCD is protected in a way to be solely used in the signature-creation process by the legitimate signatory during the validity of this SCD/SVD pair.

The TOE stores the SCD and may export the SVD. The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP).

The TOE will destroy the SCD if it is no longer used for signature generation.

When in usage phase, the TOE allows the creation of a new SCD/SVD pair. The previous SCD shall be destroyed before the creation of the new SCD/SVD pair.

Copyright Axalto SA – 2008.

The signatory uses a signature-creation system to create electronic signatures. The signature-creation device consists in the TOE.
The SCA presents the DTBS to the signatory and prepares the DTBS-representation that the signatory wishes to sign for performing the cryptographic function of the signature.
The TOE returns the secure electronic signature.

The electronic signature is supported by the security object system, depicted in the next section.

2.2.2.2 Secondary services, partially included in the evaluation scope

Additionally to the electronic signature, the TOE offers some support services for this evaluated function and some other services that are not intended to be evaluated. These services are represented in: the evaluated ones in black text, the others in grey text and dashed line outlined.

1. The TOE is able to import, store, and export data thanks to specific APDUs. This function is based on the security object system. It supports the electronic signature, which makes it part of the evaluation scope, but also other functions that are not inside the evaluation scope.
2. The data received may be decrypted by the TOE. This is not part of the evaluation scope.
3. The keys for such deciphering operations are imported in the TOE during Personalization or through a trusted channel and stored in the TOE. This is not part of the evaluation scope.

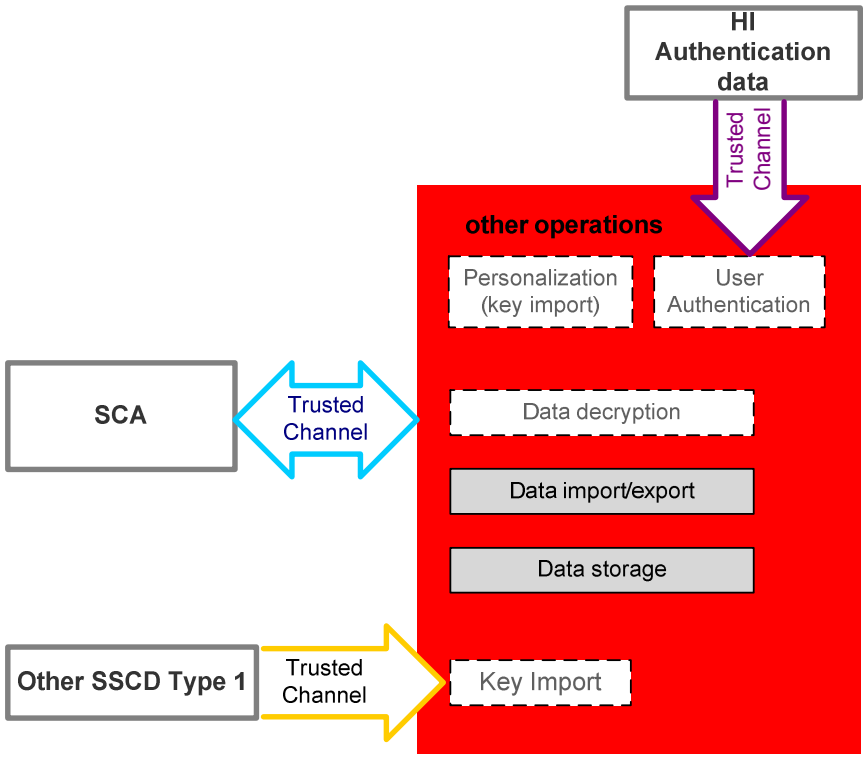

Figure 2.3 – Support operations inside and outside evaluation scope

Copyright Axalto SA – 2008.

2.3 TOE intended usage

The use cases are depicted in the following figure. The main use case is the electronic signature. Some other use cases are possible, but as they are based on non-evaluated functions (see previous §2.2.2.2 and the related use cases in §2.3.3 hereafter), the applications and the data flow are marked with dashed lines.

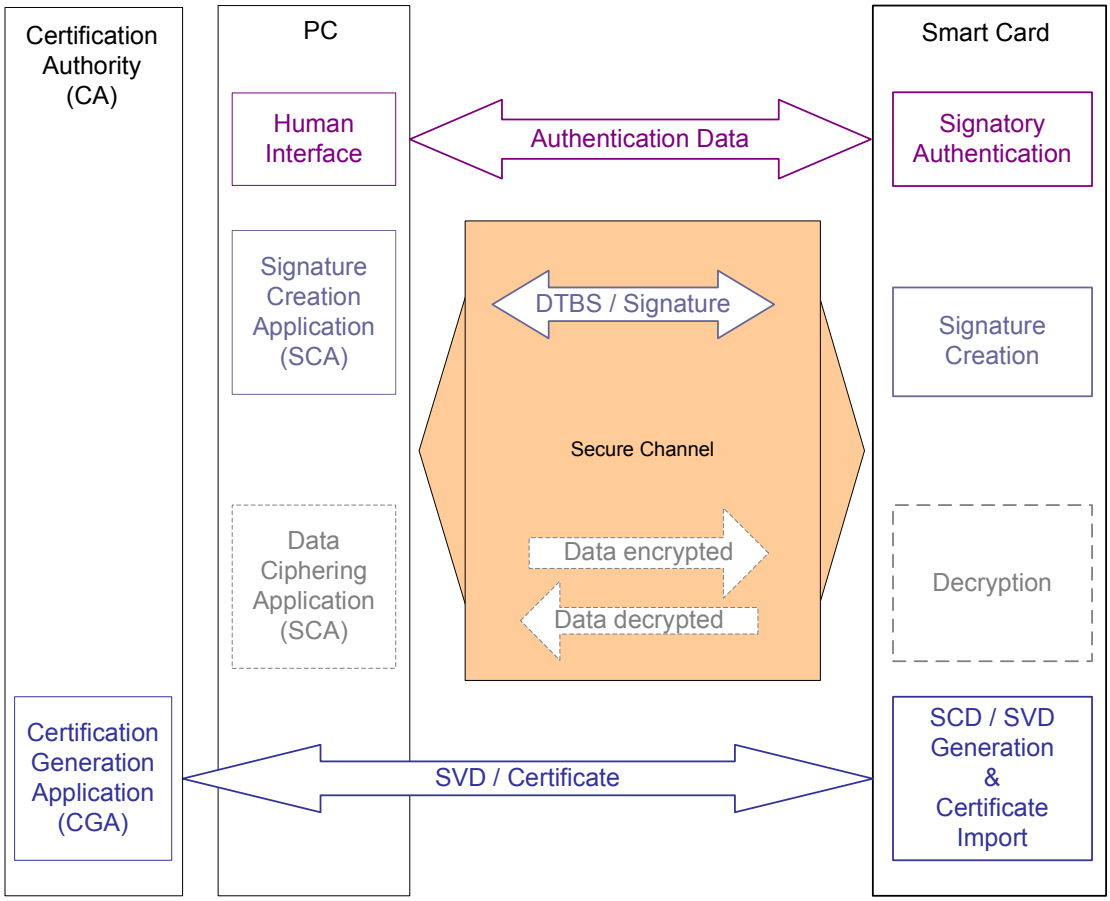

Figure 2.4 – TOE Usage

The product guidance provides additional information on the TOE administration, configuration or usage. Please refer to [ADM_ODYSSEUS] (especially chapter 9 and partially 10) or [USR_ODYSSEUS] (especially chapter 4 and partially 6). For instance, the optional secure channel between card and PC may be used to protect operations as signature and decryption unless the environment ensures equivalent protection. Also, [ADM_ODYSSEUS] refers to [PERS_ODYSSEUS][3] in chapter 9, document that provides the minimum IAS personalisation in order to obtain a SSCD configuration.

2.3.1 Evaluated main use cases: Signature

SCD/SVD Key generation in the final usage phase,

The SCA authenticates itself to the TOE.
The signatory enters its PIN code.
The signatory requests the generation of a SCD / SVD key pair
The SCD / SVD is generated in the TOE.
The SVD is sent to the CGA.

[3] [ADM_ODYSSEUS] internal reference is "[IAS_Perso]".

Copyright Axalto SA – 2008.

The CGA generates the certificate and sends it to the TOE.
Signature Creation in the final usage phase,
The SCA authenticates itself to the TOE.
The signatory enters its PIN code.
The signatory sends the DTBS to the TOE.
The TOE computes the Signature.
The TOE sends the Signature to the SCA.

2.3.2 Evaluated support use cases: Security object system

The card manages a security object system allowing management of access conditions, and cryptographic operations. It is implemented using Security Data Objects (SDO). There is a particular type of SDO which is the security environment saved in EEPROM. They are holding the card security policy.

The card is able to import, store and export security object in the security object system.
Especially signatory security objects are stored for authentication.

2.3.3 Use cases outside the evaluation scope

2.3.3.1 File system use cases

The card manages a file system allowing file creation, modification and deletion. The supporting file types are: Master File (MF), Dedicated File (DF) and Elementary transparent File (EF).

The supported operations on DF files are: creation, selection and deletion.
On EF file, the supported operations are: read binary, update binary, file selection and file deletion.

The card is able to import, store and export data in the file system. The information stored in files is mainly used for signatory identification.

2.3.3.2 Ciphering and deciphering use cases

The card offers a deciphering service using an asymmetric key set [RSA]:
- The SCA initializes secure channel with the TOE,
- The signatory enters its PIN code,
- The data is sent to be deciphered from the PC to the TOE.
- The TOE deciphers the data and sends back the data to the PC through the secure channel.
- Then the PC is able to use the data.

Copyright Axalto SA – 2008.

2.4 Smart Card Product Life-cycle

The product life cycle is described in the following picture:

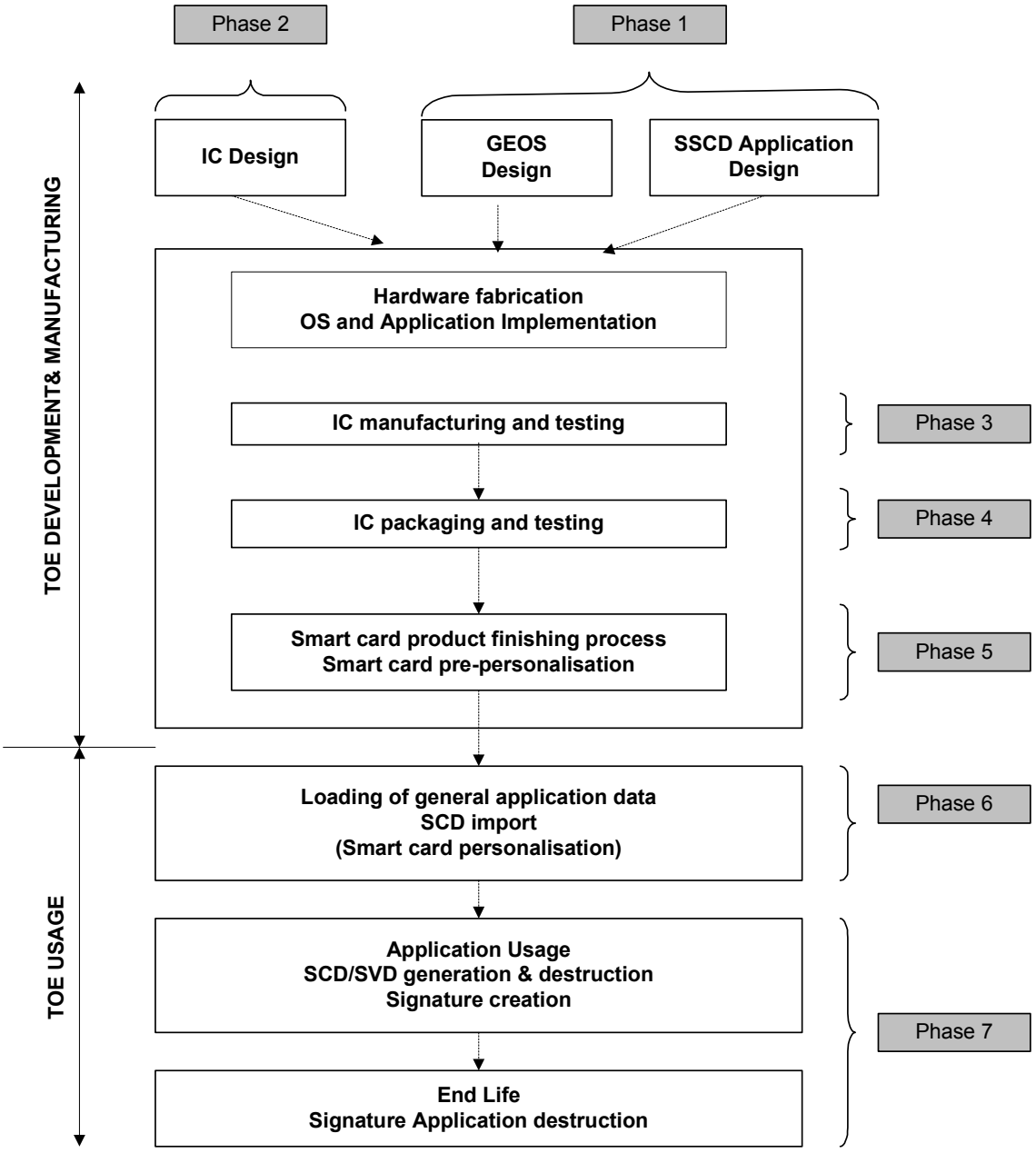

Figure 2.5 – Life Cycle

The TOE is the product at the end of phase 5 as shown in.
OS design and **application design** correspond to life phase 1 "Smart card software development".
Hardware design corresponds to life phase 2 "IC development".
Hardware fabrication OS and Application implementation correspond to life phase 3 "IC manufacturing and testing", phase 4 "IC packaging and testing", phase 5 "Smart card product finishing process".

Copyright Axalto SA – 2008.

Loading of general application data and **SCD import (type 2)** corresponds to life phase 6 "Smart card personalization".
SCD/SVD generation and Signature creation (type 3) correspond to life phase 7 "Smart card usage".
SSCD destruction corresponds to the end of life phase 7.

The global security requirements of the TOE mandate to consider, during the development phase, the threats to security occurring in the other phases. This is why this ST addresses the functions used in phases 6 and 7 but developed during phases 1 to 5.
The limits of the evaluation process correspond to phases 1 to 5 including the TOE under development delivery from the party responsible of each phase to the parties responsible of the following phases.
These different phases may be performed at different sites. This implies that procedures on the delivery process of the TOE must exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to 5 to subsequent phases, including:

Intermediate delivery of the TOE or the TOE under construction within a phase,
Delivery of the TOE or the TOE under construction from one phase to the next.

These procedures must be compliant with the security assurance requirements developed in TOE "Security Assurance Requirements" section.

The following table gives a description of the product life cycle and explains where the authorities are involved:

Phase 1	Smart Card OS development	The Embedded Software developer is responsible for the development of the Operating System and the specification of initialisation requirements (OS options).
Phase 2	IC design, IC database construction and IC photomask fabrication (IC & DS development)	The IC manufacturer is responsible for these operations, taking as an input the embedded software data given by Embedded Software developer.
Phase 3	IC manufacturing and testing	The IC manufacturer is responsible for producing and testing the IC through three main steps: IC manufacturing, testing, and IC pre-personalisation.
Phase 4	Die bonding. Microelectronic testing.	The IC packaging manufacturer is responsible for die bonding and microelectronic testing. The transport key is changed to Gemalto key.
Phase 5	Smart card product finishing process	The smart card product manufacturer is responsible for the smart card product finishing process, to install the application (if needed) and testing, and the smart card pre-personalization (including the application installation, if needed).
Phase 6	Smart card Personalization	The Personaliser is responsible for the Smart Card personalization and for final tests.
Phase 7	Smart card operational-usage	The smart card issuer is responsible for the smart card product delivery to the smart card end-user, and for the end of life process.

2.5 TOE Environment

Considering the TOE, four types of environment are defined:

1. Development and fabrication environment (phase 1 to 4),
2. Initialisation environment corresponding to smart card pre-personalization (phase 5) the loading of TOE application data and the import of the SCD (phase 6),
3. User environment, during which the card generates the signatures on behalf of the end user. The card also destructs and generates SCD/SVD pairs (phase 7),

Copyright Axalto SA – 2008.

4. End of life environment, during which the TOE is made inapt for the signature creation (end of the phase 7).

2.5.1 TOE Development & Production Environment

The TOE described in this ST is developed in different places as indicated below:

IC design	Infineon München
Secure OS Design	Gemalto Meudon
IAS application design	Gemalto Meudon
PrePersonalization design	Gemalto Meudon
IC manufacturing and Testing	Infineon München
IC packaging and testing	Gemalto Orleans or Gemenos
PrePersonalization	Gemalto Orleans or Gemenos

In order to ensure security, the environment in which the development takes place must be made secure with access control tracing entries. Furthermore, it is important that all authorized personnel feels involved and fully understands the importance and the rigid implementation of the defined security procedures.
The development begins with the TOE specification. All parties in contact with sensitive information are required to abide by Non-disclosure Agreement.
Design and development of the ES then follows. The engineers use a secure computer system (preventing unauthorised access) to make the conception, design, implementation and test performances.
Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).
Testing, programming and deliveries of the TOE then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.
During the electronic transfer of sensitive data, procedures must be established to ensure that the data arrive, only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies). It must also be ensured that transfer is done without modification or alteration.
During fabrication, phases 3, and 4, all the persons involved in storage and transportation operations should fully understand the importance of the defined security procedures.
Moreover, the environment in which these operations take place must be secured.
The TOE Initialisation is performed in [Infineon München phase 3; Gemalto Orléans or Gemenos phase 4 & 5].
In the initialisation environment of the TOE, smart card pre-personalization takes place (phase 5).
During smart card pre-personalisation the application data structure is created.
The initialisation requires a secure environment, which guarantees the integrity and confidentiality of operations.

2.5.2 TOE User Environment

In the usage environment, the personalization takes place (phase 6). Additional data may be loaded and the SCD may be imported. Then the TOE is issued to the end User.
Once delivered to the end user (phase 7), the TOE can generate the SCD/SVD key pair. The TOE then exports the public part of the key to the Certification Authority for certification.
The TOE is owned by the end user imposing strict security rules. It is the responsibility of the TOE and of the signature protocols to ensure that the signature security requirements are met.

Copyright Axalto SA – 2008.

2.5.3 End of life Environment.

End of life must be considered for several reasons:

- The SCD can be compromised,
- The TOE can be stolen,
- The TOE physical support can come to the end of its useful life.

In all these cases, it must be ensured that the TOE cannot be used any more for signature creation.

2.5.4 The actors and roles

The actors can be divided in:

Product Developers

The IC designer and DS developer designs the chip and its Dedicated Software (DS). Here it is INFINEON.
The Embedded Software Developer designs the Operating System (OS) according to IC and DS specifications. Here it is GEMALTO.

Product Manufacturer

The IC manufacturer -or founder- designs the photomask, manufactures the IC with its Dedicated Software and hardmask from the Product Developer. Here the founder and IC manufacturer is INFINEON.
The IC die bounding manufacturer is responsible for the die bounding from the ICs provided by the founder. For this product, the die bounding manufacturer is GEMALTO.
The Smart Card product manufacturer (or Card manufacturer) is responsible to obtain a pre-personalized card from a packaged IC. For this product, the Smart Card product manufacturer is GEMALTO.

Personalizer

The Smart Card Personalizer personalizes the card by loading two categories of data:

1. additional code belonging to the Developer and Manufacturer of the Card (softmask);
2. the Cardholder data as well as cryptographic keys and PINs.

The Personalizer may also load card issuer applets during this phase. Here it is GEMALTO.

Phase	**Administrator**	**Environment**
6	Smart Card Personalizer	Production Environment

At the end of this phase, only applets may be loaded. The card is issued in OP_SECURED state.

Card Issuer, Administrator

The Card Issuer -short named "issuer"- is a National Administration (or Identity Cards Authority). It issues cards to the citizens who are the "Cardholders". The Card Issuer has also the role of Administrator. Therefore, the Card Issuer is responsible for selecting and managing the personalization, for managing applets (load, install and delete), for creating the Signatory's PIN, for optionally importing the first SCD into the TOE, as well as for distribution and invalidation of the card.

End User, Signatory

The Signatory is the End-User in the usage phase (phase 7). S/He owns the TOE.
The card is personalized with the Cardholder identification and secrets.
The Signatory can sign, destroy the SCD and generate a new SCD/SVD pair.
At the first usage of the TOE, the Signatory must change his PIN code before he is allowed to sign. A new PIN is also required each time a new SCD/SVD pair is generated.

The roles (administration and usage) are defined in the following tables. During the delivery between phases the responsibility is transferred from the current phase administrator to the next phase administrator.

Copyright Axalto SA – 2008.

Phase	Administrator	Environment
6 and 7	Card Issuer	Personalization and Usage Environment

Phase	User	Environment
7	End User	Usage Environment

2.5.5 TOE Intended Usage

The TOE intended usage is the creation of Secure Signatures of data and Data ciphering and deciphering.
The TOE also stores the credential and keeps it confidential.
The TOE also stores also user information and keeps it confidential.

Copyright Axalto SA – 2008.

3 TOE security environment

3.1 Assets

The assets of the TOE are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3], [PP/JCS] and [PP/BSI-0002]. This Security Target deals with the assets of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. The assets of [PP/JCS] are studied in [ST_ODYSSEUS-PLTF]. The assets of [PP/BSI-0002] are studied in [ST/Infineon].

3.1.1 SSCD

D.SCD

Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

D.SVD

The public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).

D.DTBS

DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (their integrity must be maintained).

D.VAD

PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed).

D.RAD

Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained).

D.SSCD

Signature-creation function of the SSCD using the SCD: the quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.

D.SIG

Electronic signature: unforgeabilty of electronic signatures must be assured.

3.2 Subjects

3.2.1 SSCD

S.User

End user of the TOE which can be identified as S.Admin or S.Signatory.

Copyright Axalto SA – 2008.

S.Admin

User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.

S.Signatory

User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

S.OFFCARD

Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level potential attack and knows no secret**.

3.3 Assumptions

The Assumptions of the TOE are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3], [PP/JCS] and [PP/BSI-0002].
The present Security Target deals with the Assumptions of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].
The Assumptions of [PP/JCS] are studied in [ST_ODYSSEUS-PLTF].
The Assumptions of [PP/BSI-0002] are studied in [ST/Infineon].

3.3.1 SSCD

These are the assumptions from [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

A.CGA

Trustworthy certification-generation application.

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA

Trustworthy signature-creation application.

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.SCD_Generate

Trustworthy SCD/SVD generation.

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

(a) this party will use a SSCD for SCD/SVD-generation,

(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.

(d) The generation of the SCD/SVD is invoked by authorised users only

(e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported.

Copyright Axalto SA – 2008.

3.3.2 Additional

These are assumptions additional to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

A.Key_Mngt

Secure Key Management

The IT Environment SCA and CGA shall protect the confidentiality of the keys used for the secure communications with the TOE.

3.4 Threats

The Threats of the TOE are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3], [PP/JCS] and [PP/BSI-0002].
The present Security Target deals with the Threats of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].
The Threats of [PP/JCS] are studied in [ST_ODYSSEUS-PLTF].
The Threats of [PP/BSI-0002] are studied in [ST/Infineon].

3.4.1 SSCD

T.Hack_Phys

Physical attacks through the TOE interfaces.

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises.

T.SCD_Divulg

Storing, copying, and releasing of the signature-creation data.

An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive

Derive the signature-creation data.

An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery

Forgery of the electronic signature

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud

Repudiation of signatures.

If an attacker can successfully threaten any of the assets, then the non repudation of the electronic signature is compromised.

Copyright Axalto SA – 2008.

The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery

Forgery of the signature-verification data.

An attacker forges the SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.

T.DTBS_Forgery

Forgery of the DTBS-representation.

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.

T.SigF_Misuse

Misuse of the signature-creation function of the TOE.

An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

3.5 Organisational security policies

3.5.1 SSCD

P.CSP_QCert

Qualified certificate.

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures.

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

P.Sigy_SSCD

TOE as secure signature-creation device.

The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

Copyright Axalto SA – 2008.

4 Security objectives

4.1 Security objectives for the TOE

The TOE Objectives are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3], [PP/JCS] and [PP/BSI-0002].
The present Security Target deals with the Objectives of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].
The Objectives of [PP/JCS] are studied in [ST_ODYSSEUS-PLTF].
The Objectives of [PP/BSI-0002] are studied in [ST/Infineon].

4.1.1 SSCD

This section describes the TOE objectives of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

OT.SCD_Unique is an environment objective in Type 2.

OT.EMSEC_Design

Provide physical emanations security.

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security

Lifecycle security.

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation or re-import.

OT.SCD_Secrecy

Secrecy of the signature-creation data.

The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD.

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

OT.SVD_Auth_TOE

TOE ensures authenticity of the SVD.

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

OT.Tamper_ID

Tamper detection.

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

Copyright Axalto SA – 2008.

OT.Tamper_Resistance

Tamper resistance.

The TOE prevents or resists physical tampering with specified system devices and components.

OT.SCD_Transfer

Secure transfer of SCD between SSCD.

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

OT.DTBS_Integrity_TOE

Verification of the DTBS-representation integrity.

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBSrepresentation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

OT.Sigy_SigF

Signature generation function for the legitimate signatory only.

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.Sig_Secure

Cryptographic security of the electronic signature.

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.SCD_Unique

Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

Application note:

Type 3 TOE Objective.

OT.Init

SCD/SVD generation

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorised users only.

Application note:

This is a Type 3 Objective.

4.2 Security objectives for the environment

The Environment Objectives are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3], [PP/JCS] and [PP/BSI-0002].

Copyright Axalto SA – 2008.

The present Security Target deals with the Objectives of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].
The Objectives of [PP/JCS] are studied in [ST_ODYSSEUS-PLTF].
The Objectives of [PP/BSI-0002] are studied in [ST/Infineon].

4.2.1 SSCD

The Objectives are those of Type 2 and Type 3 from PP/SSCD.

OE.SCD_SVD_Corresp

Correspondence between SVD and SCD

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer

Secure transfer of SCD between SSCD

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

OE.SCD_Unique

Uniqueness of the signature-creation data

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context "practically occur once" means that the probability of equal SCDs is negligible low.

OE.CGA_QCert

Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA

CGA verifies the authenticity of the SVD

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.HI_VAD

Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.SCA_Data_Intend

Copyright Axalto SA – 2008.

Data intended to be signed

The SCA

(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

(b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

4.2.2 Additional

These are environment objectives additional to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

OE.Key_Mngt

Secure management of the keys

The IT Environment SCA and CGA protect the confidentiality of the keys used for the secure communications with the TOE.

Copyright Axalto SA – 2008.

5 IT security requirements

5.1 TOE security functional requirements

5.1.1 SSCD

5.1.1.1 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation** and specified cryptographic key sizes **1536 and 2048 bits** that meet the following: **none (generation of random numbers and Miller-Rabin primality testing)**.

Application note:

Type 3 only.

FCS_CKM.4/SCD Cryptographic key destruction

FCS_CKM.4.1/SCD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physical irreversible destruction of the stored key value** that meets the following: **no standard**.

Application note:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator.

The destruction of the SCD is mandatory before the SCD is re-imported into the TOE.

Type 2 (re-importation of SCD) and Type 3 (regeneration of a new SCD).

FCS_COP.1/CORRESP Cryptographic operation

FCS_COP.1.1/CORRESP The TSF shall perform **SCD / SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA key computation** and cryptographic key sizes **1536 or 2048 bits** that meet the following: **no standard**.

Copyright Axalto SA – 2008.

FCS_COP.1/SIGNING Cryptographic operation

FCS_COP.1.1/SIGNING The TSF shall perform **digital signature-generation** in accordance with a specified cryptographic algorithm **[RSA_SHA_PKCS#1]** and cryptographic key sizes **1536 or 2048 bits** that meet the following: **[RSA PKCS#1]**.

5.1.1.2 User data protection (FDP)

Access control (FDP_ACC.1)

FDP_ACC.1/Initialisation SFP Subset access control

FDP_ACC.1.1/Initialisation SFP The TSF shall enforce the **Initialisation SFP** on **Generation of SCD by User**.

Application note:

Type 3 only.

FDP_ACC.1/SVD Transfer SFP Subset access control

FDP_ACC.1.1/SVD Transfer SFP The TSF shall enforce the **SVD Transfer SFP** on **import and on export of SVD by User**.

Application note:

FDP_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

FDP_ACC.1/SCD Import SFP Subset access control

FDP_ACC.1.1/SCD Import SFP The TSF shall enforce the **SCD Import SFP** on **import of SCD by User**.

FDP_ACC.1/Personalisation SFP Subset access control

FDP_ACC.1.1/Personalisation SFP The TSF shall enforce the **Personalisation SFP** on **creation of RAD by Administrator**.

FDP_ACC.1/Signature-creation SFP Subset access control

FDP_ACC.1.1/Signature-creation SFP The TSF shall enforce the **Signature-creation SFP** on

Copyright Axalto SA – 2008.

1. **sending of DTBS-representation by SCA,**
2. **signing of DTBS-representation by Signatory**.

Security attributes (FDP_ACF.1)

The security attributes for the user, TOE components and related status are:

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialisation attribute group		
User	SCD / SVD management	authorised, not authorised
SCD	secure SCD import allowed	no, yes
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorised SCA	no, yes

(see table in PP in §5.1.2.2 Security attribute based access control)

FDP_ACF.1/Initialisation SFP Security attribute based access control

FDP_ACF.1.1/Initialisation SFP The TSF shall enforce the **Initialisation SFP** to objects based on the following: **General attribute and Initialisation attribute**.

FDP_ACF.1.2/Initialisation SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to generate SCD/SVD pair**.

FDP_ACF.1.3/Initialisation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Initialisation SFP The TSF shall explicitly deny access of subjects to objects based on the **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair**.

Application note:

Type 3 only.

Copyright Axalto SA – 2008.

FDP_ACF.1/SVD Transfer SFP Security attribute based access control

FDP_ACF.1.1/SVD Transfer SFP The TSF shall enforce the **SVD Transfer SFP** to objects based on the following: **General attribute**.

FDP_ACF.1.2/SVD Transfer SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD**.

FDP_ACF.1.3/SVD Transfer SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SVD Transfer SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

Application note:

FDP_ACF.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_ACF.1/SCD Import SFP Security attribute based access control

FDP_ACF.1.1/SCD Import SFP The TSF shall enforce the **SCD Import SFP** to objects based on the following: **General attribute and Initialisation attribute group**.

FDP_ACF.1.2/SCD Import SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes"**.

FDP_ACF.1.3/SCD Import SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SCD Import SFP The TSF shall explicitly deny access of subjects to objects based on the **(a) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".**

(b) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

Application note:

Type 2 only.

Copyright Axalto SA – 2008.

FDP_ACF.1/Personalisation SFP Security attribute based access control

FDP_ACF.1.1/Personalisation SFP The TSF shall enforce the **Personalisation SFP** to objects based on the following: **General attribute**.

FDP_ACF.1.2/Personalisation SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **User with the security attribute "role" set to "Administrator" is allowed to create the RAD**.

FDP_ACF.1.3/Personalisation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Personalisation SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

FDP_ACF.1/Signature-creation SFP Security attribute based access control

FDP_ACF.1.1/Signature-creation SFP The TSF shall enforce the **Signature-creation SFP** to objects based on the following: **General attribute and Signature-creation attribute group**.

FDP_ACF.1.2/Signature-creation SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes"**.

FDP_ACF.1.3/Signature-creation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Signature-creation SFP The TSF shall explicitly deny access of subjects to objects based on the **(a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".**

(b) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

Export of User Data (FDP_ETC.1)

FDP_ETC.1/SVD Transfer Export of user data without security attributes

FDP_ETC.1.1/SVD Transfer The TSF shall enforce the **SVD Transfer SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.

Copyright Axalto SA – 2008.

FDP_ETC.1.2/SVD Transfer The TSF shall export the user data without the user data's associated security attributes.

Application note:

FDP_ETC.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

Import of User Data (FDP_ITC.1)

FDP_ITC.1/SCD Import of user data without security attributes

FDP_ITC.1.1/SCD The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/SCD The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **SCD shall be sent by an authorised SSCD**.

Application note:

A SSCD of Type 1 is authorised to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 are able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

Type 2 only.

FDP_ITC.1/DTBS Import of user data without security attributes

FDP_ITC.1.1/DTBS The TSF shall enforce the **Signature-creation SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/DTBS The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/DTBS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **DTBS-representation shall be sent by an authorised SCA**.

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

Copyright Axalto SA – 2008.

Residual Information Protection (FDP_RIP.1)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD, VAD, RAD**.

Stored data integrity monitoring and action (FDP_SDI.2)

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

1. SCD

2. RAD

3. SVD (if persistent stored by TOE).

FDP_SDI.2/Persistent Stored data integrity monitoring and action

FDP_SDI.2.1/Persistent The TSF shall monitor user data stored within the TSC for **integrity error** on all objects, based on the following attributes: **integrity checked persistent stored data**.

FDP_SDI.2.2/Persistent Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data

2. inform the Signatory about integrity error.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored within the TSC for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data

2. inform the Signatory about integrity error.

Global refinement:

The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data".

Basic data exchange confidentiality (FDP_UCT.1)

Copyright Axalto SA – 2008.

FDP_UCT.1/Receiver Basic data exchange confidentiality

FDP_UCT.1.1/Receiver The TSF shall enforce the **SCD Import SFP** to be able to **receive** objects in a manner protected from unauthorised disclosure.

Application note:

Type 2 only.

Data exchange integrity (FDP_UIT.1)

FDP_UIT.1/SVD Transfer Data exchange integrity

FDP_UIT.1.1/SVD Transfer The TSF shall enforce the **SVD Transfer SFP** to be able to **transmit** user data in a manner protected from **insertion and modification** errors.

FDP_UIT.1.2/SVD Transfer The TSF shall be able to determine on receipt of user data, whether **insertion and modification** has occurred.

Non editorial refinement:

SVD Transfer SFP will be required only if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_UIT.1/TOE DTBS Data exchange integrity

FDP_UIT.1.1/TOE DTBS The TSF shall enforce the **Signature-creation SFP** to be able to **receive** user data in a manner protected from **insertion, modification and deletion** errors.

FDP_UIT.1.2/TOE DTBS The TSF shall be able to determine on receipt of user data, whether **deletion, modification and insertion** has occurred.

5.1.1.3 Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **block RAD**.

Copyright Axalto SA – 2008.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **RAD**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

1. Identification of the user by means of TSF required by FIA_UID.1.

2. Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD import.

3. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.

4. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

"Local user" mentioned in component *FIA_UAU.1.1* is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by *FTP_TRP.1/SCA* and *FTP_TRP.1/TOE*.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

1. Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD import.

2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.

3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.4 Security management (FMT)

Copyright Axalto SA – 2008.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **signature-creation function** to **Signatory**.

FMT_MSA.1/Administrator Management of security attributes

FMT_MSA.1.1/Administrator The TSF shall enforce the **SCD Import SFP and Initialisation SFP** to restrict the ability to **modify** the security attributes **SCD / SVD management and secure SCD import allowed** to **Administrator**.

Application note:

The SCD Import SFP enforcing comes from Type 2.

The Initialisation SFP enforcing comes from Type 3.

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signature-creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **Signatory**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3/Type2 Static attribute initialisation

FMT_MSA.3.1/Type2 The TSF shall enforce the **SCD Import SFP and Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Non editorial refinement:

The security attribute of the SCD "SCD operational" is set to "no" after import of the SCD.

FMT_MSA.3.2/Type2 The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Type3 Static attribute initialisation

FMT_MSA.3.1/Type3 The TSF shall enforce the **Initialisation SFP and Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Non editorial refinement:

Copyright Axalto SA – 2008.

The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.

FMT_MSA.3.2/Type3 The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify** the **RAD** to **Signatory**.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator and Signatory**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.1.5 Protection of the TSF (FPT)

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests **during initial start-up** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Global refinement:

In this document, the underlying abstract machine test is the IC and its library.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC FPT_EMSEC.1.1 The TOE shall not emit **Side channel current** in excess of **State of the art limits** enabling access to **RAD and SCD**.

FPT_EMSEC.1.2 The TSF shall ensure **all users** are unable to use the following interface **external contacts** to gain access to **RAD and SCD**.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed.

Copyright Axalto SA – 2008.

Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **power shortage, over and under voltage, over and under clock frequency, over and under temperature, integrity problems**.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **voltage, clock frequency and temperature out of bounds as well as penetration attacks** to the **integrated circuit** by responding automatically such that the TSP is not violated.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up and at the conditions when calling a sensitive module** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **the TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

FTP_ITC.1/SCD Import Inter-TSF trusted channel

FTP_ITC.1.1/SCD Import The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Copyright Axalto SA – 2008.

FTP_ITC.1.2/SCD Import The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD Import [Editorially Refined] The TSF or the trusted IT shall initiate communication via the trusted channel for **SCD import**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD of type 1.

Application note:

Type 2 only.

FTP_ITC.1/SVD Transfer Inter-TSF trusted channel

FTP_ITC.1.1/SVD Transfer The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD Transfer The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD Transfer [Editorially Refined] The TSF or the trusted IT shall initiate communication via the trusted channel for **transfer of SVD**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD of type 1 for SVD import and the CGA for the SVD export.

Application note:

FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

FTP_ITC.1/DTBS Import Inter-TSF trusted channel

FTP_ITC.1.1/DTBS Import The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/DTBS Import The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

Non editorial refinement:

The remote trusted IT product is the SCA.

FTP_ITC.1.3/DTBS Import [Editorially Refined] The TSF or the SCA shall initiate communication via the trusted channel for **signing DTBS-representation**.

Copyright Axalto SA – 2008.

FTP_TRP.1/TOE Trusted path

FTP_TRP.1.1/TOE The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2/TOE The TSF shall permit **local users** to initiate communication via the trusted path.

FTP_TRP.1.3/TOE The TSF shall require the use of the trusted path for **initial user authentication**.

5.1.2 Additional

This SFR is added for compliancy with CC version 2.3, it misses from the PP.

5.1.2.1 Security management (FMT)

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **Identification and authentication management, access condition management**.

5.2 TOE security assurance requirements

The security assurance requirement level is EAL4. The EAL is augmented with AVA_MSU.3, AVA_VLA.4, ADV_IMP.2 and ALC_DVS.2.

5.3 Security requirements for the IT environment

5.3.1 IT environment functional requirements

5.3.1.1 SSCD

SSCD Type1

This group comes from Type 2 only and therefore applies only for it. The TSF in this section is the IT environment (the TSF of a SSCD Type1 TOE).

FCS_CKM.1/Type1 Cryptographic key generation

FCS_CKM.1.1/Type1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation** and specified cryptographic key sizes **1536 or 2048 bits** that meet the following: **none (generation of random numbers and Miller-Rabin primality testing)**.

Copyright Axalto SA – 2008.

FCS_CKM.4/Type1 Cryptographic key destruction

FCS_CKM.4.1/Type1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physical irreversible destruction of the stored key value** that meets the following: **no standard**.

Application note:

The cryptographic key SCD will be destroyed automatically after export.

FCS_COP.1/CORRESP-Type1 Cryptographic operation

FCS_COP.1.1/CORRESP-Type1 The TSF shall perform **SCD / SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA key computation** and cryptographic key sizes **1536 or 2048 bits** that meet the following: **no standard**.

FDP_ACC.1/SCD Export SFP Subset access control

FDP_ACC.1.1/SCD Export SFP The TSF shall enforce the **SCD Export SFP** on **export of SCD by Administrator**.

FDP_UCT.1/Sender Basic data exchange confidentiality

FDP_UCT.1.1/Sender The TSF shall enforce the **SCD Export SFP** to be able to **transmit** objects in a manner protected from unauthorised disclosure.

FTP_ITC.1/SCD Export Inter-TSF trusted channel

FTP_ITC.1.1/SCD Export The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCD Export The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD Export [Editorially Refined] The TSF or the SSCD Type2 shall initiate communication via the trusted channel for **SCD export**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD Type2.

Copyright Axalto SA – 2008.

Application note:

If the SSCD Type 1 exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the SSCD Type 1 and the SSCD Type 2 will be required.

Certification generation application (GGA)

FCS_CKM.2/CGA Cryptographic key distribution

FCS_CKM.2.1/CGA The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **qualified certificate** that meets the following: **Triple DES 112 bits**.

FCS_CKM.3/CGA Cryptographic key access

FCS_CKM.3.1/CGA The TSF shall perform **import the SVD** in accordance with a specified cryptographic key access method **import through a secure channel** that meets the following: **no standard**.

FDP_UIT.1/SVD Import Data exchange integrity

FDP_UIT.1.1/SVD Import The TSF shall enforce the **SVD import SFP** to be able to **receive** user data in a manner protected from **modification and insertion** errors.

FDP_UIT.1.2/SVD Import The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

FTP_ITC.1/SVD Import Inter-TSF trusted channel

FTP_ITC.1.1/SVD Import The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD Import The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD Import [Editorially Refined] The TSF or the remote trusted IT product shall initiate communication via the trusted channel for **import SVD**.

Signature creation application (SCA)

Copyright Axalto SA – 2008.

FCS_COP.1/SCA Hash Cryptographic operation

FCS_COP.1.1/SCA Hash The TSF shall perform **hashing the DTBS** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **[FIPS 180-2], length = 160 bits**.

FDP_UIT.1/SCA DTBS Data exchange integrity

FDP_UIT.1.1/SCA DTBS The TSF shall enforce the **Signature-creation SFP** to be able to **transmit** user data in a manner protected from **modification, deletion and insertion** errors.

FDP_UIT.1.2/SCA DTBS The TSF shall be able to determine on receipt of user data, whether **deletion, modification and insertion** has occurred.

FTP_ITC.1/SCA DTBS Inter-TSF trusted channel

FTP_ITC.1.1/SCA DTBS The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCA DTBS The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCA DTBS [Editorially Refined] The TSF or the remote trusted IT product shall initiate communication via the trusted channel for **signing DTBS-representation by means of the SSCD**.

FTP_TRP.1/SCA Trusted path

FTP_TRP.1.1/SCA The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2/SCA The TSF shall permit **the TSF** to initiate communication via the trusted path.

FTP_TRP.1.3/SCA The TSF shall require the use of the trusted path for **initial user authentication**.

Copyright Axalto SA – 2008.

5.4 Security requirements for the non-IT environment

5.4.1 Non-IT environment functional requirements

5.4.1.1 SSCD

R.Administrator_Guide Application of Administrator Guidance

The implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensures the ongoing compliance.

R.Sigy_Guide Application of User Guidance

The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name Signatory's name in the Qualified Certificate

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD which stores the SCD corresponding to the SVD to be included in the qualified certificate.

Copyright Axalto SA – 2008.

6 TOE summary specification

6.1 TOE security functions

The minimum strength for the security functions is SOF-high.

6.1.1 SSCD

This is the group of SF which is specific to the SSCD.

SF.KeyGen

Key generation

The TOE shall generate an RSA key pair for Digital Signature: 1536 and 2048 bit-long modulus product of 2 large prime numbers.

The generation ensures the proof of consistency between SCD and SVD.

SF.Sig

Signature creation

TOE shall be able to sign a hash of data imported from outside the card.

The TOE shall use an RSA_SHA1_PKCS#1 signature scheme with a 1536 or 2048 bit-long modulus.

The signature function shall have an access condition based upon previous authentication of user.

SF.SecMes

Secure Messaging

This function establishes a secure channel between the interface device (IFD) and the smartcard. It allows protecting the confidentiality (ENC) and the data authentication and integrity (SIG) of data transmitted to and from the card. It is used to ensure the DTBS integrity prior performing signature creation.

- ENC operations use triple TDES with 2 keys, in ECB mode.
- MAC operations use triple TDES with 2 keys, in CBC mode.

DTBS: if an integrity error is found, an error flag is raised, the corresponding data is made unavailable and the corresponding operation is aborted.

SF.RAD/VAD management

RAD/VAD Management for application

This SF controls all the operations relative to the RAD/VAD management, including the Cardholder (signatory) authentication:

- RAD creation: the RAD is stored and is associated to a maximum sucessful presentation number (usage counter) and to a maximum error number.
- VAD verification: the RAD can be accessed only if its format and integrity are correct and if the usage counter has not reached 0. If the RAD is blocked, then it cannot be used anymore.
- RAD ratification counter: The number of authentication attempts is limited by a counter associated to the RAD. The counter is decremented each time the VAD verification fails. The RAD cannot be used any longer if the counter reaches zero.

Copyright Axalto SA – 2008.

- RAD usage counter: the usage counter is decremented each time the RAD is verified successfully. When this counter reaches 0, the RAD cannot be verified anymore.
- RAD modification: the RAD can be changed by the cardholder (loading a new value). The RAD is managed and stored by the application. The operations on RAD and VAD are performed thanks to services offered by the platform using by the javacard.framework.OwnerPin class.

This SF uses probabilistic mechanisms.

The strength of this function is SOF-high.

SF.ExtAuth

External Authentication

This function authenticates an external entity.

This function checks the candidate authenticity and controls that it corresponds to its identity before giving him the authorization attached to it. It is an external authentication using symmetric (TDES) or asymmetric (RSA) cryptography.

There is a single authorization attached to each {Identity, authenticity} pair performed thanks SDO ID.

In case of symmmetric authentication, the ratification counter limits the number of authentication attempts. The counter is decremented each time the authentication fails. The authentication mechanism is blocked and cannot be used any longer if the counter reaches zero.

6.1.2 Platform

This group of SF is part of the SF provided by the platform [ST_ODYSSEUS-PLTF]. Hereafter are listed only those SF that offer support to the SSCD.

6.1.2.1 Card Operation

SF.SmartCardPlatform

As defined in [ST_ODYSSEUS-PLTF].

Application note:

Regarding the JavaCard objects belonging to the SSCD, this function provides the ability to check the integrity of:

- Cryptographic keys including SCD & SVD,
- Authentication data including RAD.

SF.CardManager

As defined in [ST_ODYSSEUS-PLTF].

6.1.2.2 Common services

SF.Transaction

As defined in [ST_ODYSSEUS-PLTF].

6.1.2.3 Java Card

SF.Erase

Copyright Axalto SA – 2008.

As defined in [ST_ODYSSEUS-PLTF].

Copyright Axalto SA – 2008.

7 PP claims

Protection Profile - Secure Signature-Creation Device

7.1 PP reference

Type2	Type 3
BSI-PP-0005-2002	BSI-PP-0006-2002
Version 1.04-EAL4+	Version 1.05 EAL4+
03.04.2002	03.04.2002

7.2 PP tailoring

Refinements of [PP/JCS] are described in [ST_ODYSSEUS-PLTF] and are not repeated here. Refinements of [PP/BSI-0002] are described in [ST/Infineon] and are not repeated here. The table below shows the functional requirements refined in PP and in ST.

Copyright Axalto SA – 2008.

Functional requirement	Refined in [PP/SSCD-TYPE2]	Refined in [PP/SSCD-TYPE3]	Refined inST
FCS_CKM.1		_	x
FCS_CKM.4	_	_	x
FCS_COP.1	x	x	x
FDP_ACC.1	x	x	(x)
FDP_ACF.1	x	x	x
FDP_ETC.1	x	x	(x)
FDP_ITC.1	x	x	(x)
FDP_RIP.1	x	x	(x)
FDP_SDI.2	x	x	(x)
FDP_UCT.1	x		(x)
FDP_UIT.1	x	x	(x)
FIA_AFL.1	x	x	x
FIA_ATD.1	x	x	(x)
FIA_UAU.1	x	x	x
FIA_UID.1	x	x	x
FMT_MOF.1	x	x	(x)
FMT_MSA.1	x	x	(x)
FMT_MSA.2	NA	NA	NA
FMT_MSA.3	x	x	(x)
FMT_MTD.1	x	x	(x)
FMT_SMR.1	x	x	(x)
FPT_AMT.1	_	_	x
FPT_EMSEC.1	_	_	x
FPT_FLS.1	_	_	x
FPT_PHP.1	NA	NA	NA
FPT_PHP.3	_	_	x
FPT_TST.1	_	_	x
FTP_ITC.1	x	x	(x)
FTP_TRP.1	x	x	x

The functional requirements are both refined in the claimed PP and in this ST. This section demonstrates the compatibility of the refinements done in both documents.

_: No refinement

(x): no additional refinement has been made in the ST.

Copyright Axalto SA – 2008.

NA: the functional requirement requires no refinement.

FMT_SMF functional requirement is added to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] to be compliant with [CC-2].

Copyright Axalto SA – 2008.

8 Rationale

8.1 Environment rationale

Not delivered in public version.

8.2 Security objectives rationale

Not delivered in public version.

8.3 Security requirements rationale

Not delivered in public version.

Copyright Axalto SA – 2008.

Notice

This document has been generated with TL SET version 1.7.1 (Trusted Logic).

Copyright Axalto SA – 2008.

Index

Copyright Axalto SA – 2008.

END OF SECURITY TARGET

Copyright Axalto SA – 2008.